

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

NO. 5:13-CV-328-FL

UNITED STATES OF AMERICA,)
)
 v.)
)
NIKHIL NILESH SHAH,)
)
 Defendant.)
)

ORDER

This matter comes before the court on the government’s motion in limine for pretrial determination of the admissibility of certain evidence. (DE 52). The court, in large part, orally ruled on the government’s motion at hearing, with such rulings confirmed by written order entered May 29, 2015. However, the court reserved ruling on the admissibility of certain electronic evidence obtained from Google, Inc. (“Google”), sought to be authenticated under Federal Rule of Evidence 902(11), pending further consideration of the parties’ briefing and arguments raised at hearing. The issues raised are now ripe for ruling. For the reasons stated below, the government’s motion, as it relates to the documents at issue, is denied.

BACKGROUND

Defendant formerly was an Information Technology Manager at Smart Online, Inc. (“SOLN”), a mobile application development company in Durham, North Carolina. Defendant left SOLN for similar employment in early 2012. On June 28, 2012, after defendant no longer was a SOLN employee, an intruder accessed the SOLN computer network and caused significant damage.

On June 29, 2012, the Durham Police Department initiated an investigation into the June 28,

2012, intrusion. This investigation later was joined by the FBI. As part of that investigation, on November 5, 2012, a United States Magistrate Judge issued a Secured Communications Act (“SCA”), 18 U.S.C. §§ 2701, et seq., warrant. As relevant here, that warrant allowed law enforcement to access certain records associated with email address SHAHNN28@GMAIL.COM, an email address allegedly used by defendant, stored locally on Google’s premises.

Law enforcement used that warrant to obtain more than one gigabyte of data associated with the email address at issue, with such information spanning from March 6, 2007, to November 2012. The data supplied by Google discussed subjects ranging from an email sent on June 29, 2012, from SHAHNN28@GMAIL.COM to SHAHNN28@GMAIL.COM, “with no subject line . . . [and] contain[ing] three website links related to. . . . firewall configurations . . . used by SOLN in its network infrastructure,” United States v. Shah, No. 5:13-CR-328-FL-1, 2015 WL 72118 (E.D.N.C. Jan. 6, 2015), to electronic chats by the user of GMail account SHAHNN28@GMAIL.COM with others, discussing intimate or otherwise sensitive topics.

On December 17, 2013, a grand jury returned a one-count indictment charging defendant with intentional damage to a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(B)(I), and 1030(c)(4)(A)(i)(I). On June 30, 2014, defendant filed three motions to suppress, among other things, the emails and chats obtained from Google pursuant to the SCA warrant, contending that those documents were obtained in violation of the Fourth Amendment to the United States Constitution. On January 6, 2015, the court entered order denying each motion. Shah, 2015 WL 72118.

On April 22, 2015, the government filed the instant motion seeking a “pretrial determination of admissibility of certain evidence.” (DE 52). Included with the government’s motion were 44

emails and chats obtained from Google, which are illustrative of the exhibits the government will seek to admit at trial. The government proffers the documents on the ground that they contain statements of a party opponent, which are excluded from the hearsay rule under Federal Rule of Evidence 801(d)(2)(A). The government seeks to authenticate those statements as if they were Google's business records, pursuant to Federal Rule of Evidence 902(11). In response, defendant argues the emails and chats are not Google's business records, and that the government may not side-step its obligation to lay foundation for and authenticate those documents at trial.

COURT'S DISCUSSION

A. Authenticity under Rule 902(11)

The government requests a pretrial ruling on the authenticity of certain emails and chats. As the proponent of the evidence, the government bears the burden to establish its admissibility. See United States v. Vidacak, 553 F.3d 344, 349 (4th Cir. 2009). As discussed above, these documents were obtained from Google, pursuant to a SCA warrant. They contain statements originating from SHAHNN28@GMAIL.COM and statements by others.

The government contends the subject documents, including the statements at issue, do not require authenticating testimony, because their authenticity is supported by the affidavit of Despina Fafoutis, Google's records custodian, (the "Google affidavit"), as required by Rule 902(11). (DE 52-47). In the Google affidavit, Fafoutis avers that Google automatically copies the information, entered by a GMail user into his or her own private emails or chats, to Google's servers at the time such email or chat is sent.¹ Fafoutis further declares that such data collection is a regularly

¹At hearing, the government's attorney expanded on this practice. Google's business model requires the collection and analysis of user data. Google collects data entered by its subscribers into web searches, emails, chats, etc. Google then analyzes such data for content and

conducted activity, and that the record is kept in the course of Google's regularly conducted business. For the reasons that follow, the court holds that the government has not met its burden of proving that these documents are Google's business records, as is required under Rule 902.

1. General Principles of Authenticity

"Before admitting evidence for consideration by the jury, the district court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic." United States v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992). Thus, authenticity itself is a question of fact for the jury, with the district court's role as that of gatekeeper, utilizing the conditional relevancy standard. See id. at 1370-71. See generally Fed. R. Evid. 104(b). Rule 902, however, creates an exception to the general rule governing authentication of evidence. If evidence falls into a category enumerated under Rule 902, "no extrinsic evidence of authenticity [is required] in order [for that evidence] to be admitted." Fed. R. Evid. 902.

The government relies on Rule 902(11) to support its theory of admissibility. That Rule states that no extrinsic evidence of authenticity is required to admit "[t]he original or copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute." Fed. R. Evid. 902(11). Thus, *per se* authenticity, as established by Rule 902(11), requires the government to demonstrate that the emails and chats at issue properly would be admissible as Google's business records. See Fed. R. Evid. 803(6).

targets advertisements toward individual subscribers based on the content of their electronic communications. The court does not rely on this information, but only recalls it here to provide context.

2. Documents at Issue as Business Records

The specific provisions of Rule 803(6) referenced in Rule 902(11) provide:

A record of an act, event, condition, opinion or diagnosis [may be admitted] if: (A) the record was made at or near the time by - - or from information transmitted by - - someone with knowledge; (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation or calling, whether or not for profit; [and] (C) making the record was a regular practice of that activity.

Fed. R. Evid. 803(6)(A) through (C). Interpreting those requirements, the Fourth Circuit recently has stated :

For a record to be admitted as a business record, it must be 1) made by a regularly conducted business activity, 2) kept in the regular course of that business, 3) the regular practice of that business to make the memorandum, 4) and made by a person with knowledge or from information transmitted by a person with knowledge.

United States v. Cone, 714 F.3d 187, 219 (4th Cir. 2013) (citing Clark v. City of L.A., 650 F.2d 1033, 1036-37 (9th Cir. 1981)). Upon consideration of the foregoing factors, the court concludes the Google affidavit fails the fourth prong of the Cone analysis, because these documents were not “made by a person with knowledge.”

The “knowledge” requirement ensures trustworthiness in the records of a regularly conducted business activity. See Certain Underwriters at Lloyd’s v. Sinkovich, 232 F.3d 200, 204-05 (4th Cir. 2000) (“[B]usinesses depend on such records to conduct their own affairs; accordingly, the employees who generate them have a strong motive to be accurate and none to be deceitful.”); see also McCormick on Evid. § 290. If any person in the chain of those contributing to the creation of the final business record is not acting in the regular course of business, then that essential element of trustworthiness fails. See Sinkovich, 232 F.3d at 205; McCormick, supra. Accordingly, “if information going from observation to final recording is to be received under [the business record]

exception, all parts of the process must be in the regular course of business.” McCormick, supra; accord United States v. Santos, 201 F.3d 953, 965 (7th Cir. 2000) (holding documents created by third parties, but kept and retained by corporation in the regular course of business inadmissible under business record exception); United States v. Patrick, 959 F.2d 991, 1001-02 (D.C. Cir. 1992) (holding portion of receipt showing defendant’s address not admissible as business record, where information was provided by third party and not verified by the business), abrogation on other grounds recognized by, United States v. Webb, 255 F.3d 890 (D.C. Cir. 2001).

The statements at issue are not Google’s business records, as that term is defined under Rule 803(6), because they fail the “knowledge” requirement. See Cone, 714 F.3d at 219. Neither SHAHNN28@GMAIL.COM, nor any other originating source whose statements appear in the records produced by Google were under a “business duty” to convey accurate information in their correspondence. Because the proffered “finished product” is not the collective effort of “business insiders,” who share a duty to ensure the accuracy of their statements, the court cannot allow those statements to be authenticated on the theory that they are Google’s self-proving business records under Federal Rules of Evidence 803(6) and 902(11). See Sinkovich, 232 F.3d at 205. To do so would unhinge the business record exception from its theoretical underpinnings of accuracy, continuity, and regularity. See Id.; McCormick, supra § 286.

Moreover, although courts have developed an exception to the “knowledge” requirement, which applies where a business independently verifies information provided to it by a third-party, see Patrick, 959 F.2d at 1001-02, such exception is not relevant to the case at bar. As illuminated at hearing by government counsel, Google’s business model does not depend on the veracity of the information contained in its stored communications. Rather, Google’s lifeblood is the mere

transmission of such information, divorced from concerns about its accuracy.

Because the documents were not created by someone “with knowledge,” as required by Rule 803(6), the court’s Rule 902(11) authenticity inquiry must end. Although these statements may well be attributable to both defendant and others, their admissibility turns on an evidentiary theory beyond that allowed by the text of Rule 902(11). Where the government proffers these statements as self-proving business records, the court may not expand its inquiry to encompass other matters. See Fed. R. Evid. 902(11) (Records admissible where they “meet[] the requirements of Rule 803(6)(A)-(C)”). Accordingly, to admit these emails and chats the government must lay foundation demonstrating that the content falls into some other exception to or exclusion from the hearsay rule.²

The court’s discussion should not be confused with an admonition that the documents may never be accepted into evidence as Google’s business records. To the contrary, upon a sufficient

²At hearing, the government contended the statements contained in the documents were made by computer, rather than by person, where Google’s computer systems copy text entered into emails and chats by users. Then, citing United States v. Washington, 498 F.3d 225 (4th Cir. 2007), the government suggests no outsider information was used in the creation of these putative “business records.” Washington is inapposite to the issue presently before the court. In that case, the Fourth Circuit held that statements automatically generated by computer, without human input, were not hearsay because they were not made by a person. See Washington, 498 F.3d at 231. Considering the statements as non-hearsay does not bring the government as far as it would hope. As noted in the text, Federal Rule of Evidence 902(11) only allows for the self-authentication of documents that meet the requirements of Rule 803(6)(A) through (C). Arguing that the statements at issue are not hearsay does nothing to advance that point. Moreover, to the limited extent the government suggests Washington may be read to support the proposition that the statements at issue do not run afoul of Rule 803(6)’s “knowledge” requirement, because they are attributable to a computer, the court is wholly unpersuaded. As noted by both the Washington court, and in all the cases cited in support of the Fourth Circuit’s conclusion, the rule in Washington is limited to circumstances where information is generated “instantaneously by . . . computer without the assistance or input of a person.” United States v. Hamilton, 413 F.3d 1138, 1142-43 (10th Cir. 2005). Here, the statements copied by Google’s servers originated with a Gmail subscriber, thus rendering the reasoning of Washington and other similar cases inapplicable.

showing that the statements made therein are statements of a party opponent, see generally Fed. R. Evid. 801(d)(2)(A), the government may introduce the Google affidavit into evidence for the purpose of establishing these documents as Google's business records.³ Thus, the court's analysis is semantic in nature and, in practice, does not operate to the detriment of the government.

2. Authenticity under Rule 901

Because the statements in the documents are not Google's business records, the government must produce evidence to authenticate such statements at trial. See Fed. R. Evid. 901(a); United States v. Branch, 970 F.2d at 1370-71. As noted earlier, the documents contain statements linked to SHAHNN28@GMAIL.COM, as well as statements originating from other sources.

With regard to the statements made by SHAHNN28@GMAIL.COM, the government's object is to connect these statements to defendant and offer them into evidence as statements of a party opponent. Fed. R. Evid. 801(d)(2)(A). To do so, it is incumbent upon the government to introduce evidence connecting defendant to the statements in order to establish their relevance. Evidence is relevant if it has any tendency to make a fact in consequence more or less probable than it would be without the evidence. Fed. R. Evid. 401. Although the government contends the emails bear heavily on the ultimate issue of defendant's guilt, special problems of authenticity inherent in electronic communications prevent the relevance of the documents proffered by the government from being readily apparent. See Fed. R. Evid. 901 advisory committee notes ("Authentication and

³ As noted at hearing, without more, the affidavit of the Google employee making reference to a coded disc is insufficient to establish that the printed, paper documents tendered by the government are in fact Google's business records. There must be some showing by a person with knowledge that, when electronically read and printer processed, the particular disc referred to by Google's affiant in fact produces the individual documents on which the government would seek to rely in this case.

identification represent a special aspect of relevancy); see also McCormick, supra § 212.

The government may not rely exclusively on defendant's prior use of the email address SHAHNN28@GMAIL.COM to authenticate the documents. Both email and electronic chats are faceless means of communication, with users identified by an email address or username. The recipient cannot, simply by looking at the email address or username provided in the document, readily identify the true identity of a message's sender. Even where the email address or username employed by the sender is an eponym, as likely is the case here, the sender's identity is not immediately discernable. In neither case can the recipient rely on the use of an email address or username to conclude that a third party has not made surreptitious use of an otherwise familiar account. Instead, the recipient must use additional information gleaned from context, for example, the knowledge that the communication was prompted by the recipient, or content, the identifying or unique characteristics inherent in the message, to identify the sender.

Because of these issues, when faced with evidence of electronic communications, courts have demanded a somewhat more stringent showing than would be required in the face of "ordinary" evidence. See United States v. Hassan, 742 F.3d 104, 133-34 (4th Cir. 2014) (holding no abuse of discretion where trial court required the government to connect electronic records to defendant's email and IP address); United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (affirming admission of defendant's email into evidence where email contained an email address known to be used by defendant, contained defendant's signature, and the content of the emails demonstrated knowledge by the sender of both defendant's criminal activity and personal relationships). Commentators, too, have recognized this limitation inherent in electronic communications, and have recommended authentication through testimony tying the "contents,

substance, internal patterns, or other distinctive characteristics . . . [as well as] the circumstances” under which the email was sent to the putative sender. Fed. R. Evid. 901(b)(4); Weinstein’s Federal Evid. § 900.07[3][c][i].

Accordingly, before these documents may be introduced into evidence the government must make sufficient showing that the context surrounding or content of these emails and chats connects defendant to them. Once the government makes such showing, the emails and chats still will be subject to ordinary evidentiary principles. See generally, e.g., Fed. R. Evid. 403.

Finally, with regard to the government’s theory supporting the admissibility of the statements of others contained in the documents, the government contends such statements fall outside the rule against hearsay, where they are not offered for the truth of the matter asserted. See Fed. R. Evid. 801(c). Rather, the government takes the position that these statements are admissible to place defendant’s statements in context.

Hearsay is a statement made outside of court offered into evidence to prove the truth of the matter asserted in the statement. Fed. R. Evid. 801(c). It follows that, where a statement is offered for some purpose other than the truth of its subject matter, the hearsay rule will not bar its admission.

In United States v. Wills, 346 F.3d 476 (2003), the Fourth Circuit held that statements of third parties are admissible as non-hearsay where they are “reasonably required to place [defendant’s] responses [to those statements] in context.” Id. at 489-90. The court reasoned that third-party statements may be necessary to make any incriminating admissions “intelligible to the jury and recognizable as admissions.” Id. at 490 (quoting United States v. Lemonakis, 485 F.2d 941, 948 (D.C. Cir. 1973)).

Based on the reasoning in Wills, the third-party statements at issue generally may be

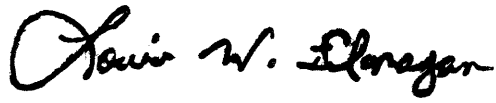
admissible. However, the Wills rule, as well as other independent evidentiary principles, do not allow for the *per se* admissibility of all such statements. Instead, the government should endeavor to minimize the use of third-party statements in its effort to prove context. As noted, those statements are admissible only where they are reasonably required to make any putative incriminating statement clear to the jury. Wills, 346 F.3d at 490-91. While a showing of strict necessity is not required, if context is not “reasonably required” for this purpose, questions regarding the relevancy of third-party statements arise. See Fed. R. Evid. 401.

In sum, the government’s motion seeking a pretrial ruling on the authenticity of certain emails obtained from Google pursuant to a SCA warrant, under Federal Rule of Evidence 902(11) is denied. The documents are not Google’s business records, as that term is defined in Rule 803(6), because the operative statements contained therein were not made by an individual with “knowledge.” Because the government has not carried its burden under 902(11), it must lay foundation for these exhibits as statements of a party opponent at trial. To do so, the government must offer sufficient evidence connecting defendant to the content of or context surrounding the documents sent by the user of SHAHNN28@GMAIL.COM.

CONCLUSION

Based on the foregoing, the government’s motion in limine, (DE 52) is DENIED insofar as it requests a pretrial ruling of the emails and chats, produced by Google pursuant to a SCA warrant, under Federal Rule of Evidence 902(11). The documents may not be authenticated by affidavit alone, and require foundation to be established at trial pursuant to Federal Rule of Evidence 901.

SO ORDERED, this the 5th day of June, 2015.

A handwritten signature in black ink, reading "Louise W. Flanagan". The signature is written in a cursive style with a large initial "L".

LOUISE W. FLANAGAN
United States District Judge